Minicurso

Códigos detectores e corretores de erros: uma introdução

Victor do Nascimento Martins

Universidade Federal da Bahia
Programa de Verão do IME-UFBA 2024
Semana temática de Álgebra e Topologia Algébrica
29 a 31 de janeiro de 2024

RESUMO

Neste minicurso abordaremos de forma abrangente diversos aspectos relacionados aos códigos corretores de erros. Iniciaremos com a definição fundamental de códigos, contextualizando seu papel na detecção e correção de erros em transmissões de dados. Ao explorar o contexto histórico, destacaremos marcos importantes no desenvolvimento desses códigos ao longo do tempo. A apresentação de exemplos práticos ilustrará a aplicação concreta desses códigos em diferentes domínios. Dentre os tópicos a serem abordados, dedicaremos atenção especial aos códigos lineares e códigos cíclicos, explorando suas propriedades e aplicações. Além disso, forneceremos uma breve visão das áreas de pesquisa de cientistas brasileiros, incluindo códigos de grupo, códigos algébricos geométricos, códigos e reticulados, destacando a contribuição nacional para o avanço nesse campo crucial da teoria da informação.

Alegre, ES, Janeiro de 2024.

Victor do Nascimento Martins
(*victor.n.martins@ufes.br*)
Departamento de Matemática Pura e Aplicada
Centro de Ciências Exatas, Naturais e da Saúde
Universidade Federal do Espírito Santo (Campus de Alegre)

SUMÁRIO

INTRODUÇÃO

Os códigos corretores de erros estão em praticamente todo sistema de envio de informações que conhecemos, como assistir um vídeo no Youtube, mandar mensagem pelo Whatsapp ou ao fazer uma ligação por exemplo. Trata-se de uma maneira organizada de transmitir uma mensagem, isto é, nos permite ao receber uma informação, que seja possível detectar e corrigir erros, garantindo segurança ao usuário.

A necessidade de transmitir informações de maneira confiável e precisa sempre foi uma preocupação ao longo da história, impulsionando o desenvolvimento de tecnologias que garantam a integridade dos dados. A história da teoria dos códigos corretores de erros nos revela como esses mecanismos se tornaram fundamentais na era digital.

O embrião dos códigos corretores de erros pode ser rastreado até as comunicações militares durante a Segunda Guerra Mundial. Naquele contexto, as mensagens enviadas por rádio muitas vezes eram sujeitas a interferências e ruídos, resultando em informações distorcidas ou perdidas. Para superar esse desafio, os militares começaram a explorar técnicas para detectar e corrigir erros nas mensagens, garantindo a entrega precisa das informações.

A teoria surgiu no final dos anos 40, quando o matemático americano C. E. Shanon, do Laboratório Bell, se questionou sobre o porque as máquinas não eram capazes de encontrar a posição de um determinado erro e corrigí-lo, uma vez que elas podiam detectá-lo. A década de 1940 testemunhou o surgimento dos primeiros códigos de detecção de erros, como o código de Hamming, proposto por Richard Hamming em 1950. Esse código foi uma pedra fundamental no desenvolvimento dos códigos corretores de erros, pois não apenas detectava erros, mas também fornecia informações para corrigi-los.

Com o avanço da computação e o aumento da complexidade nas comunicações digitais, os códigos corretores de erros evoluíram. Durante as missões espaciais, como as do programa

Apollo nas décadas de 1960 e 1970, a NASA adotou esses códigos para garantir a transmissão confiável de dados entre a Terra e as espaçonaves.

À medida que a tecnologia da informação se tornava onipresente na sociedade, os códigos corretores de erros se tornaram essenciais em várias aplicações. Em discos rígidos, memórias RAM, transmissões de dados por redes sem fio e ópticas, esses códigos desempenham um papel crucial na prevenção e correção de erros.

Hoje, vivemos em um mundo onde a comunicação digital é a espinha dorsal de muitas atividades cotidianas. Os códigos corretores de erros continuam a desempenhar um papel vital, garantindo que nossos dados sejam transmitidos e armazenados de maneira confiável. Essa contextualização histórica destaca não apenas a evolução técnica desses códigos, mas também sua importância duradoura na sociedade, cada vez mais tecnológica.

Vejamos um exemplo familiar de um código corretor de erros. Vamos considerar um idioma. Seja $\mathcal{A}$ o alfabeto brasileiro. Vamos denotar por $\mathcal{P}$ o conjunto das palavras da língua portuguesa. Uma palavra da língua portuguesa pode ser considerada um elemento de $\mathcal{A}^{46}$, onde 46 é a quantidade de letras da maior palavra de $\mathcal{P}$, a saber, *pneumoultramicroscopicos-silicovulcanoconiótico*[1]. Agora, note que $\mathcal{P}$, é um subconjunto próprio de $\mathcal{A}^{46}$, o que faz com que esse código seja detector e corretor de erros. De fato, suponha que ao enviar a mensagem "saudade" ocorresse alguma interferência de modo que a palavra recebida foi, na verdade, "sautade". Como essa palavra não pertence a $\mathcal{P}$, percebe-se imediatamente que houve erro, e corrigí-lo é muito simples, já que a palavra em $\mathcal{P}$ que mais se aproxima de "sautade" é "saudade".

Agora suponha que ao enviar a mensagem "gato" ocorra erro em que a mensagem recebida seja "rato". Diferente do exemplo anterior, a detecção desse erro será muito dificil, já que "rato" também pertence a $\mathcal{P}$. Contudo, suponha que depois de certo esforço foi possível detectar a existência de um erro. Um pensamento natural seria pensar em como corrigí-lo, o que também não seria tarefa fácil, porque existem mais palavras em $\mathcal{P}$ que se parecem com "gato", como por exemplo as palavras "tato", "nato" e "pato". Isso acontece porque um idioma não é um código muito eficiente, pois nele existem palavras muito "próximas" uma das outras.

No decorrer deste trabalho iremos esclarecer o que queremos dizer com proximidade entre as palavras de um código. Para isso, dividimos este material em três capítulos. O primeiro dedicado a teoria básica, onde apenas temos o propósito de solidificar o conceito de código e apresentar os primeiros objetos matemáticos da teoria. No segundo capítulo iremos introduzir estruturas algébricas para apresentar os códigos lineares e uma classes destes:

[1]Com 46 letras, a palavra foi registrada em 2001 no dicionário Houaiss e descreve o indivíduo que possui doença pulmonar causada pela inspiração de cinzas vulcânicas. FONTE: BBC News Brasil

os códigos cíclicos. Nessa oportunidade iremos mostrar como a utilização das estruturas de espaços vetoriais e anéis aumentarão nossas ferramentas para lidar com os processos de codificação. Por fim, no Capítulo 3 iremos apresentar um pouco cobre algumas vertentes da área de códigos corretores de erros que vêm se desenvolvendo no Brasil e traremos alguns nomes de pesquisadores brasieliros que estão contribuindo significativamente nos estudos da teoria.

Esperamos com este texto apenas motivar o leitor a se aprofundar no estudo das teorias aqui apresentadas, portanto, iremos fazer indicações de referências mais completas sobre todos os tópicos aqui apresentados.

CAPÍTULO 1

TEORIA BÁSICA DE CÓDIGOS

Neste capítulo inicial esperamos elucidar de maneira mais objetiva o que é um código corretor de erros através de um exemplo simples e em seguida apresentaremos os primeiros objetos matemáticos da teoria que utilizaremos. A importante noção de distância entre palavras de um código será apresentada. Para mais detalhes sugerimos uma leitura do Capítulo 1 de (HEFEZ; VILLELA, 2008).

1.1 Código: conceito e exemplos

Um código corretor de erros é um mecanismo utilizado em comunicações digitais para detectar e corrigir erros que possam ocorrer durante a transmissão de dados. Ele desempenha um papel crucial na garantia da integridade das informações transmitidas, especialmente em ambientes propensos a interferências, ruídos ou outras formas de degradação do sinal.

A ideia fundamental por trás dos códigos corretores de erros é a introdução de redundância nos dados transmitidos. Isso significa adicionar informações extras aos dados originais de modo que, se ocorrer um erro durante a transmissão, o receptor possa identificar e corrigir esse erro automaticamente.

Um exemplo histórico notável do uso de códigos corretores de erros ocorreu durante a missão Apollo 11, em 1969, quando a NASA enviou os primeiros seres humanos à lua. As comunicações entre a Terra e a espaçonave Apollo eram cruciais, e a transmissão de dados, como imagens e telemetria, precisava ser confiável. Para garantir isso, foram implementados códigos corretores de erros nas transmissões.

Outro exemplo relevante ocorre em sistemas de transmissão de imagens do espaço, como

o envio de fotos de sondas espaciais para a Terra. Um dos métodos mais comuns para garantir a integridade dessas imagens é a utilização de códigos de correção de erros. Isso é vital porque, em ambientes espaciais, o sinal pode ser afetado por diversas formas de interferência, como radiação cósmica e outros fenômenos que podem levar a erros na transmissão.

Existem diversos tipos de códigos corretores de erros, como os códigos de Hamming, códigos Reed-Solomon, entre outros. Cada um desses códigos tem características específicas, mas todos compartilham o objetivo comum de garantir a confiabilidade na transmissão de dados.

Em resumo, os códigos corretores de erros desempenham um papel crucial em diversas áreas, desde comunicações espaciais até transmissões de dados cotidianas, garantindo que as informações cheguem ao destino de forma precisa e íntegra, mesmo em condições adversas.

Quando falamos em códigos, estamos lidando fundamentalmente com ferramentas digitais, então, nesse processo de transmissão de informações, primeiro é preciso converter essas informações em sinal digital, ou melhor, codificá-las, para só então serem transmitidas. Entretanto, assim como no código do idioma, no momento da transmissão a mensagem pode ser adulterada pela interferência de ruídos (ou erros), que se dão por causa do meio físico utilizado (computadores, celulares, etc), os chamados **canais**. Assim, os canais são melhorados para reduzir a possibilidade de ruído, evitando que eventuais erros possam surgir por causa do mal uso desses equipamentos ou até mesmo aleatoriamente. Para resolver este problema, foram traçadas algumas estratégias, a mais comum é a técnica de repetição, onde a mesma mensagem é transmitida várias vezes e depois todas as recepções são comparadas, pois elas podem ajudar na reconstrução da mensagem original. É claro que não é possível garantir que a mensagem será reconstruída corretamente todas as vezes, essa questão deve ser encarada em termos probabilísticos.

Como essas repetições são realizadas através de equipamentos físicos, elas geram custo, que pode ser entendido como o tempo gasto no processo, custo financeiro ou mesmo na capacidade dos computadores. Na verdade, as repetições só multiplicam esse custo, então é preciso encontrar um balanço entre custo e confiabilidade na transmissão, sabendo que quanto maior for a quantidade de repetições, maior será a confiança de que a mensagem será entregue corretamente, ao mesmo passo que quanto maior for a quantidade de repetições, maior será o custo.

Vejamos um exemplo mais elaborado de um código para ilustrar os princípios da teoria. Suponha um helicóptero de controle remoto, onde suas únicas direções possíveis de vôo são norte, sul, leste, oeste, sudeste, nordeste, sudoeste e noroeste. Tomando $A = \{0, 1\}$, os oito movimentos podem ser codificados em elementos de $\{0, 1\} \times \{0, 1\} \times \{0, 1\}$, como no diagrama abaixo.

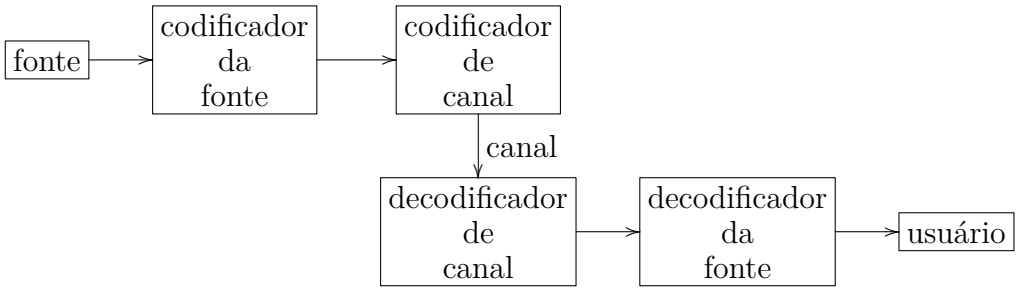
$$\begin{array}{ll} \text{Leste} \mapsto 000 & \text{Nordeste} \mapsto 110 \\ \text{Oeste} \mapsto 001 & \text{Sudeste} \mapsto 101 \\ \text{Norte} \mapsto 011 & \text{Noroeste} \mapsto 010 \\ \text{Sul} \mapsto 100 & \text{Sudoeste} \mapsto 111 \end{array}$$

O código numérico à direita é chamado de **código da fonte**. Imaginemos que ao enviar a mensagem 011, aconteça uma interferência fazendo com que a mensagem recebida seja 010, isso faria com que o helicóptero fosse para noroeste ao invés de ir para o norte. Para evitar com que isso aconteça, o que se faz é recodificar as palavras, introduzindo uma série de redundâncias que permitam detectar e corrigir erros. Agora em $\{0,1\}^6$.

$$\begin{array}{ll} \text{Leste} \mapsto 000000 & \text{Nordeste} \mapsto 110010 \\ \text{Oeste} \mapsto 001011 & \text{Sudeste} \mapsto 101110 \\ \text{Norte} \mapsto 011100 & \text{Noroeste} \mapsto 010111 \\ \text{Sul} \mapsto 100101 & \text{Sudoeste} \mapsto 111001 \end{array}$$

O novo código introduzido é chamado de **código de canal**. Suponhamos que ao se transmitir a mensagem 110010, tenha ocorrido um erro de modo que a palavra recebida foi 111010, é fácil notar que essa última não pertence ao código, portanto, a detecção do erro é possível. Comparando essa mensagem com as do código, vemos que a que "mais se aproxima" de 111010 é 110010, que é precisamente a mensagem inicialmente transmitida.

A teoria de códigos tem como objetivo transformar o código da fonte em código de canal, em detectar e corrigir erros e em decodificar o código de canal em código da fonte. Estes são os chamados processos de **codificação** e **decodificação**, e é isso que está exemplificado no diagrama a seguir:



O estudo da teoria de códigos tem como um de seus principais pilares encontrar algoritmos de codificação e decodificação cada vez melhores, por isso a ideia de mesclar códigos com estruturas algébricas é bastante promissora, uma vez que ao realizarmos códigos sobre estruturas algébricas ganhamos todas as ferramentas dessas estruturas na busca por processos de codificação e decodificação mais eficientes.

1.2 Distância de Hamming

Consideremos um conjunto finito $\mathcal{A}$ qualquer com q elementos, que será chamado **alfabeto**. Os elementos deste conjunto serão chamados de **letras** ou **dígitos**. Uma **palavra** é uma sequência de letras e o **comprimento** dessa palavra é o número de letras que a compõe.

Consideremos o conjunto $\mathcal{A}^n = \{(c_0, \ldots, c_{n-1}) : c_i \in \mathcal{A}, 0 \leq i \leq n-1\}$ de todas as palavras de comprimento n sobre $\mathcal{A}$.

Dado um número natural n qualquer, um **código** é um subconjunto próprio de $\mathcal{A}^n$.

Um importante conceito na teoria de códigos é o de distância entre as palavras. Vimos na Introdução que o conjunto de palavras da língua portuguesa não é um código muito eficiente porque nele existem palavras muito "próximas". É importante estabelecermos uma definição precisa dessa proximidade. Assim, introduzimos a seguir uma das métricas mais utilizadas na teoria: a métrica de Hamming.

Definição 1.1 *Dados dois elementos $u, v \in \mathcal{A}^n$, a **distância de Hamming** entre u e v é dada por*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|,$$

onde $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ e $|A|$ denota o número de elementos do conjunto A.

Se $\mathcal{C}$ é um código então chamamos de **distância mínima** de $\mathcal{C}$ o número

$$d = min\{d(u, v) : u, v \in \mathcal{C} \text{ e } u \neq v\}.$$

Exemplo 1.1 *Seja $\mathcal{A} = \{0, 1\}$. Considere o código $\mathcal{C} = \{0000, 0101, 1011, 1111\} \subset \mathcal{A}^4$. Vamos calcular as distâncias entre os elementos de $\mathcal{C}$.*

$$d(0000, 0101) = 2, \quad d(0000, 1011) = 3, \quad d(0000, 1111) = 4,$$

$$d(0101, 1011) = 3, \quad d(0101, 1111) = 2, \quad d(1011, 1111) = 1.$$

Logo a distância mínima de $\mathcal{C}$ é $d = 1$.

Proposição 1.1 *A distância de Hamming determina uma métrica em $\mathcal{A}^n$, ou seja, dados u, v e $w \in \mathcal{A}^n$, valem as seguintes propriedades:*

- *Positividade: $d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.*
- *Simetria: $d(u, v) = d(v, u)$.*

- *Desigualdade Triangular:* $d(u,v) \leq d(u,w) + d(w,v)$.

Demonstração:

- Por definição $d(u,v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| \geq 0$. Se $d(u,v) = 0$, temos $u_i = v_i$, para todo $i \in \{1, \ldots, n\}$ e daí $u = v$. Por outro lado se $u = v$, temos $u_j = v_j$, para $1 \leq j \leq n$ e, portanto, $d(u,v) = 0$.

- Segue direto da definição já que temos que comparar entrada por entrada de cada palavra e lembramos que a igualdade é uma relação simétrica.

- Dados u, $v \in \mathcal{A}^n$, sejam u_i, v_i as i-ésimas coordenadas de u e v. Considerando a contribuição dessas coordenadas para $d(u,v)$ temos duas situações:

1) Se $u_i = v_i$ nada acrescentaremos a $d(u,v)$ devido a essa coordenada, no entanto em $(d(u,w) + d(w,v))$ poderemos ter um acréscimo de 0 ou 2, justificando o resultado.

2) Se $u_i \neq v_i$ acrescentaremos 1 em $d(u,v)$ e ainda pelo menos uma das duas coisas acontece: $u_i \neq w_i$ ou $w_i \neq v_i$, ou seja, teremos sempre um acréscimo de no mínimo 1 em $(d(u,w) + d(w,v))$, encerrando a demonstração.
■

Definição 1.2 *Dados $c \in \mathcal{A}^n$ e $t > 0$ um número real, define-se o* ***disco*** *de centro c e raio t, respectivamente, por:*

$$D(c;t) = \{u \in \mathcal{A}^n : d(u,c) \leq t\}.$$

Lema 1.1 (Lema 1, (HEFEZ; VILLELA, 2008)) *Para todo $c \in \mathcal{A}^n$ e todo número natural $r > 0$, temos*

$$|D(c;r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Lema 1.2 *Seja $\mathcal{C}$ um código com distância mínima d. Se c e c' são palavras distintas de $\mathcal{C}$, então*

$$D(c;\kappa) \bigcap D(c';\kappa) = \emptyset$$

onde $\kappa = [\frac{d-1}{2}]$ e $[t]$ representa a parte inteira de um número real t.

Demonstração: De fato, se existisse $x \in D(c;\kappa) \bigcap D(c';\kappa)$, teríamos

$$d(x,c) \leq \kappa \quad \text{e} \quad d(x,c') \leq \kappa.$$

Daí

$$d \leq d(c, c') \leq d(c, x) + d(x, c') \leq 2\kappa.$$

Mas,

$$d - 1 = 2 \cdot \kappa + r, \qquad \text{com} \quad 0 \leq r < 2$$

e, portanto

$$d = 2 \cdot \kappa + r + 1 > 2\kappa,$$

um absurdo.

■

Teorema 1.1 *Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $\kappa = [\frac{d-1}{2}]$ erros e detectar até $d-1$ erros.*

Demonstração: Suponha que ao transmitirmos uma palavra c do código cometemos t erros com $t \leq \kappa$, recebendo a palavra r, então $d(r, c) = t \leq \kappa$. Pelo Lema 1.2, a distância de r a qualquer outra palavra do código é maior do que κ. Isso determina c univocamente a partir de r, corrigindo a palavra recebida e substituindo-a por c. Por outro lado, dada uma palavra do código, podemos nela introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. ■

Definição 1.3 *Seja $\mathcal{C} \subset \mathcal{A}^n$ um código com distância mínima d e seja $\kappa = [\frac{d-1}{2}]$. O código $\mathcal{C}$ será dito perfeito se*

$$\bigcup D(c; \kappa) = \mathcal{A}^n.$$

Uma consequência do Teorema 1.1 é que um código terá capacidade de correção de erros maior quanto maior for a sua distância mínima. Em códigos com palavras de comprimento maior é possível ter distâncias mínimas maiores. Porém, na teoria de códigos nunca devemos esquecer do custo gerado a partir do aumento de palavras ou de comprimento. Deve haver sempre uma busca pelo equilíbrio destes parâmetros.

Os **três parâmetros fundamentais** de um código $\mathcal{C} \subset \mathcal{A}^n$ são $[n; M; d]$, onde n é o comprimento do código, M o número de elementos e d a distância mínima de $\mathcal{C}$. Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros, pois veremos mais adiante que existe uma interdependência complexa entre eles.

CAPÍTULO 2

CÓDIGOS COM ESTRUTURA ALGÉBRICA

A inserção de estruturas algébricas surge como uma abordagem fundamental para aprimorar e otimizar o desempenho dos códigos corretores de erros. Ao incorporar estruturas algébricas na teoria de códigos corretores de erros, ampliamos significativamente nosso entendimento sobre os processos subjacentes à detecção e correção de erros em transmissões de dados. A abstração proporcionada pela álgebra permite a criação de modelos matemáticos elegantes que capturam a essência dos algoritmos de correção de erros, proporcionando insights valiosos para o desenvolvimento de códigos mais eficientes.

Neste capítulo, exploraremos a importância crucial de se integrar estruturas algébricas na teoria de códigos corretores de erros. Examinaremos como conceitos fundamentais da álgebra, como espaços vetoriais, anéis e corpos, oferecem uma base sólida para a formulação e análise de códigos. Iremos apresentar os códigos lineares e uma classe desses códigos que são os cíclicos. Nestes casos iremos realizar os códigos sobre as estuturas de espaço vetorial e posteriormente de anel. Para mais detalhes sugerimos (COSTA, 2022) e (HEFEZ; VILLELA, 2008).

2.1 Espaços vetoriais: códigos lineares

A partir de agora, o alfabeto do código será sempre um corpo finito $\mathbb{K}$. Desta forma, para cada n natural temos um $\mathbb{K}$-espaço vetorial $\mathbb{K}^n$ de dimensão n.

Seja $\mathcal{C} \subset \mathbb{K}^n$. Dizemos que $\mathcal{C}$ é um **código linear** se $\mathcal{C}$ é um subespaço vetorial de $\mathbb{K}^n$.

Um código linear possui 3 parâmetros principais n, k e d, que são a dimensão do espaço vetorial, a dimensão do código como subespaço vetorial e a distância mínima, res-

pectivamente. Se $\mathcal{C}$ tem dimensão k sobre $\mathbb{K}$, dizemos que $\mathcal{C}$ é um (n,k) - código linear e se $\mathcal{C}$ tem distância mínima d, dizemos que $\mathcal{C}$ é um (n,k,d) - código linear. Para a teoria de códigos, são interessantes os códigos em que k e d são relativamente grandes em relação a n.

Seja k a dimensão de um código $\mathcal{C}$ e seja $\{\mathbf{v_1},...,\mathbf{v}_k\}$ uma de suas bases, então todo elemento de $\mathcal{C}$ se escreve como combinação linear, de modo único, na forma

$$\lambda_1\mathbf{v_1} + \lambda_\mathbf{2}\mathbf{v_2} + ... + \lambda_k\mathbf{v}_k,$$

onde $\lambda_i \in \mathbb{K}$, para todo $i = 1,...,k$. Daí

$$M = |\mathcal{C}| = q^k,$$

e, conseqüentemente,

$$dim_{\mathbb{K}}\mathcal{C} = k = log_q q^k = log_q M.$$

Definição 2.1 *Dado $x = (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$, define-se o **peso** de x como sendo o número inteiro*

$$\omega(x) := |\{i : x_i \neq 0\}|.$$

Em outras palavras, $\omega(x) = d(x,0)$, onde d é a distância de Hamming.

Definição 2.2 *O **peso** de um código linear $\mathcal{C}$ é o inteiro*

$$\omega(\mathcal{C}) := min\{\omega(x) : x \in \mathcal{C}\backslash\{0\}\}.$$

Exemplo 2.1 *O código do helicóptero da Seção 1.1 é linear. Naquele caso tínhamos como alfabeto o corpo finito $\mathbb{F}_2 = \{0,1\}$. Este código pode ser realizado como imagem da transformação linear*

$$\begin{array}{rccl} T & : {\mathbb{F}_2}^3 & \longrightarrow & {\mathbb{F}_2}^6 \\ & (x_1,x_2,x_3) & \mapsto & (x_1,x_2,x_3,x_1+x_2,x_2+x_3,x_1+x_2+x_3) \end{array},$$

que é um subespaço de ${\mathbb{F}_2}^6$.

As palavras 110010 *e* 111001 *têm respectivamente pesos* 3 *e* 4 *e calculando os demais pesos das palavras deste código verificamos que este possui peso* 3.

Em um código linear $\mathcal{C}$ com distância mínima d, temos que $d(\mathbf{u},\mathbf{v}) = \omega(\mathbf{u}-\mathbf{v})$, para quaisquer $\mathbf{u},\mathbf{v} \in \mathbb{K}^n$ e, ainda, $d = \omega(\mathcal{C})$. Assim, basta efetuar $M-1$ cálculos de distâncias em um código linear com M elementos para calcularmos a distância mínima, sendo que anteriormente era preciso efetuar $\begin{pmatrix} M \\ 2 \end{pmatrix}$ cálculos de distâncias.

Utilizaremos resultados de álgebra linear para descrevermos de duas maneiras um código linear $\mathcal{C}$. Na primeira, um código $\mathcal{C}$ é visto como conjunto imagem de uma transformação linear e, na segunda, como núcleo.

Seja a base canônica $\{e_1, \ldots, e_n\}$ de $\mathbb{K}^n$, para algum n natural. Consideremos uma base $\{v_1, ..., v_k\}$ de um código $\mathcal{C} \subset \mathbb{K}^n$. Então $\mathcal{C}$ é isomorfo a $\mathbb{K}^k$. Podemos definir uma aplicação linear injetora $T : \mathbb{K}^k \longrightarrow \mathbb{K}^n$ por $T(e_i) = v_i$, para $0 \leq i \leq k$. Por construção de T vemos que $Im(T) = \mathcal{C}$.

Agora vamos descrever $\mathcal{C}$ através de uma transformação linear sobrejetora $T' : \mathbb{K}^n \longrightarrow \mathbb{K}^{n-k}$ tal que $Ker(T') = \mathcal{C}$.

Dada uma base $\{v_1, ..., v_k\}$ de $\mathcal{C}$ podemos ampliá-la a uma base $\{v_1, ..., v_k, c_1, ..., c_{n-k}\}$ de $\mathbb{K}^n$.

Seja $v \in \mathbb{K}^n$. Logo v pode ser escrito como

$$v = \lambda_1 v_1 + \ldots + \lambda_k v_k + \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}$$

onde $\lambda_i \in \mathbb{K}$, $1 \leq i \leq n$. Agora basta definirmos $T' : \mathbb{K}^n \longrightarrow \mathbb{K}^{n-k}$ por

$$v \longmapsto v' = \lambda_{k+1} c_1 + \ldots + \lambda_n c_{n-k}.$$

As aplicações T e T' podem ser visualizadas no seguinte diagrama;

$$\begin{array}{ccccc} & \overset{T}{} & & \overset{T'}{} & \\ \mathbb{K}^k & \longrightarrow & \mathbb{K}^n & \longrightarrow & \mathbb{K}^{n-k} \\ | & & | & & | \\ \mathbb{K}^k & \longrightarrow & \mathcal{C} & \longrightarrow & 0 \end{array}$$

onde $\mathcal{C} = Im(T) = Ker(T')$.

Exemplo 2.2 *Considere o corpo finito com três elementos* $\mathbb{F}_3 = \{0, 1, 2\}$ *e seja* $\mathcal{C} \subset \mathbb{F}_3^4$ *o código gerado pelos vetores* $\mathbf{v_1} = \mathbf{1011}$ *e* $\mathbf{v_2} = \mathbf{0112}$. *Esse código possui 9* $(= q^k = 3^2)$ *elementos, pois tem dimensão 2 sobre um corpo de 3 elementos. Uma representação paramétrica de* $\mathcal{C}$ *é dada por*

$$\lambda_1 \mathbf{v_1} + \lambda_2 \mathbf{v_2},$$

variando λ_1 *e* λ_2 *em* $\mathbb{F}_3$. *O código* $\mathcal{C}$ *pode ser representado como núcleo da transformação linear*

$$\begin{array}{rccc} H: & \mathbb{F}_3^4 & \longrightarrow & \mathbb{F}_3^2 \\ & (x_1, x_2, x_3, x_4) & \mapsto & (2x_1 + 2x_2 + x_3, 2x_1 + x_2 + x_4) \end{array}$$

2.1.1 Equivalência de códigos

Quando se fala em uma classe de objetos matemáticos como os códigos, é natural se pensar sobre equivalência entre eles, isto é, objetos que possuem mesmos parâmetros. A noção de equivalência de códigos lineares é baseada no conceito de isometria linear definida a seguir.

Definição 2.3 *Seja $\mathbb{K}$ um alfabeto e n um número natural, dizemos que uma aplicação linear $T : \mathbb{K}^n \to \mathbb{K}^n$ é uma **isometria** de $\mathbb{K}^n$ se*

$$d(T(\mathbf{u}), T(\mathbf{v})) = d(\mathbf{u}, \mathbf{v}), \forall \ \mathbf{u}, \mathbf{v} \in \mathbb{K}^n,$$

onde d é a distância de Hamming.

Proposição 2.1 *(i) Toda isometria de $\mathbb{K}^n$ é uma bijeção de $\mathbb{K}^n$.*

(ii) A função identidade de $\mathbb{K}^n$ é uma isometria.

(iii) Se T é uma isometria de $\mathbb{K}^n$, então T^{-1} é uma isometria de $\mathbb{K}^n$.

(iv) Se T e U são isometrias de $\mathbb{K}^n$, então $T \circ U$ é uma isometria de $\mathbb{K}^n$.

Definição 2.4 *Sejam $\mathcal{C}, \mathcal{C}'$ códigos lineares em $\mathbb{K}^n$. Dizemos que $\mathcal{C}'$ é **linearmente equivalente** a C se existir uma isometria T de $\mathbb{K}^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.*

Segue da Proposição 2.1 que a equivalência linear de códigos é uma relação de equivalência. Ou seja, é reflexiva, simétrica e transitiva. Códigos equivalentes tem os mesmos parâmetros (dimensão do espaço, dimensão do código e distância mínima).

Veremos abaixo exemplos de duas famílias importantes de isometrias.

Exemplo 2.3 *Se $f : \mathbb{K} \to \mathbb{K}$ é uma bijeção linear, e i é um número tal que $1 \leq i \leq n$, então a aplicação*

$$\begin{array}{rcl} T_f^i : \mathbb{K}^n & \to & \mathbb{K}^n \\ (c_1, \ldots, c_n) & \mapsto & (c_1, \ldots, f(c_i), \ldots, c_n) \end{array}$$

é uma isometria.

Exemplo 2.4 *Se π é uma bijeção do conjunto $\{1, \ldots, n\}$ nele prório, também chamada permutação de $\{1, \ldots, n\}$, então a aplicação permutação de coordenadas*

$$\begin{array}{rcl} T_\pi : \mathbb{K}^n & \to & \mathbb{K}^n \\ (c_1, \ldots, c_n) & \mapsto & (c_{\pi(1)}, \ldots, c_{\pi(n)}) \end{array}$$

é uma isometria.

O teorema a seguir nos dá uma caracterização das isometrias de $\mathbb{K}^n$ e, portanto, nos dá uma maneira de obter códigos equivalentes.

Teorema 2.1 *Seja $T : \mathbb{K}^n \to \mathbb{K}^n$ uma isometria. Então existem uma permutação π de $\{1, \ldots, n\}$ e bijeções lineares f_i de $\mathbb{K}$, $i = 1, \ldots, n$ tais que*

$$T = T_\pi \circ T^1_{f_1} \circ \cdots \circ T^n_{f_n}.$$

Corolário 2.1 *Sejam $\mathcal{C}$ e $\mathcal{C}'$ códigos lineares em $\mathbb{K}^n$. Então $\mathcal{C}$ e $\mathcal{C}'$ são linearmente equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e bijeções lineares $f_1, \ldots, f_n$ de $\mathbb{K}$ tais que*

$$\mathcal{C}' = \{(f_{\pi(1)}(c_{\pi(1)}), \ldots, f_{\pi(n)}(c_{\pi(n)})) : (c_1, \ldots, c_n) \in \mathcal{C}\}.$$

Observe que se $f : \mathbb{K} \to \mathbb{K}$ é linear, existe $c \in \mathbb{K}$ tal que

$$f(x) = cx, \text{ para todo } x \in \mathbb{K}.$$

Com isso, $\mathcal{C}$ é linearmente equivalente a $\mathcal{C}'$ em $\mathbb{K}^n$ se, e somente se,

$$\mathcal{C}' = \{(c_1(x_{\pi(1)}), \ldots, c_n(x_{\pi(n)})) : (x_1, \ldots, x_n) \in \mathcal{C}, c_i \in \mathbb{K}\}.$$

Isso equivale a dizer que dois códigos lineares são linearmente equivalentes se, e somente se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

- Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.
- Permutação das posições de todas as palavras do código, mediante uma permutação fixa de $\{1, \ldots, n\}$.

2.1.2 Matriz geradora de um código

O objetivo dessa seção é mostrar as vantagens que obtemos ao mesclar códigos corretores de erros com estruturas algébricas, em particular a estrutura dos espaços vetoriais.

Seja $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ uma base de um código linear $\mathcal{C}$ e considere a matriz G a seguir.

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}.$$

A matriz G é chamada de **matriz geradora** de $\mathcal{C}$ associada à base $\mathcal{B}$, e sua importância será evidenciada a seguir.

Considere a transformação linear definida por

$$\begin{aligned} T : \mathbb{K}^k &\to \mathbb{K}^n \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Se $\mathbf{c} = (c_1, \ldots, c_k)$, temos que

$$T(\mathbf{c}) = \mathbf{c}G = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k.$$

Logo $T(\mathbb{K}^k) = \mathcal{C}$. Daí, podemos considerar $\mathbb{K}^k$ como o **código da fonte**, $\mathcal{C}$ o **código do canal** e T uma **codificação**.

Lembramos que G não é univocamente determinada, pois depende da escolha da base. Observe ainda, que uma base de um espaço vetorial pode ser obtida de uma outra qualquer através de sequências de operações do tipo:

- Permutação de dois elementos da base;
- Multiplicação de um elemento da base por um escalar não nulo;
- Substituição de um elemento da base por ele mesmo somado a um múltiplo escalar de outro elemento da base.

Segue, então que duas matrizes geradoras de um mesmo código podem ser obtidas uma da outra por sequências de operações do tipo:

- (L1) Permutação de duas linhas;
- (L2) Multiplicação de uma linha por um escalar não nulo;
- (L3) Adição de um múltiplo escalar de uma linha a outra.

Com isso, dada uma matriz G qualquer cujas linhas são linearmente independentes, podemos construir um código linear $\mathcal{C}$ como imagem de uma transformação representada por essa matriz G.

Veja agora um exemplo da utilização de uma matriz geradora.

Exemplo 2.5 *Seja $\mathbb{F}_2$ o alfabeto de um código linear $\mathcal{C}$, e considere a seguinte transformação linear*

$$\begin{aligned} T : \mathbb{F}_2^3 &\to \mathbb{F}_2^5 \\ \mathbf{c} &\mapsto \mathbf{c}G. \end{aligned}$$

Seja $\mathcal{B} = \{(1,0,1,0,1),(1,1,0,1,0),(1,1,1,1,1)\} \subset \mathbb{F}_2^5$ *uma base de* $\mathcal{C}$*. Desta forma,*

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

é uma matriz geradora de um código $\mathcal{C}$ *em* $\mathbb{F}_2^5$*. Fazendo* $T((1,1,0))$*, obtemos* $(0,1,1,1,1)$ *como codificação.*

Agora, suponha que se queira decodificar a palavra $(1,0,0,0,0)$ *do código de canal, isto é, encontrar a palavra do código da fonte a qual ela corresponde por meio de* T*. Basta resolver o sistema linear*

$$(c_1, c_2, c_3)G = (1,0,0,0,0),$$

ou seja,

$$\begin{cases} c_1 + c_2 + c_3 = 1 \\ c_2 + c_3 = 0 \\ c_1 + c_3 = 0 \\ c_2 + c_3 = 0 \\ c_1 + c_3 = 0 \end{cases}$$

cuja solução é $c_1 = 1, c_2 = 1$ *e* $c_3 = 1$*.*

Para utilizar a matriz G na codificação e decodificação de palavras do código, será preciso resolver um sistema de equações que, em geral, dada uma matriz G mais complexa que essa do exemplo, pode dar muito trabalho, é nesse sentido que damos a próxima definição.

Definição 2.5 *Seja* G *uma matriz geradora de um código linear* $\mathcal{C}$*. Dizemos que* G *está na* ***forma padrão*** *se*

$$G = (Id_k \mid A),$$

onde Id_k *é a matriz identidade* $k \times k$ *e* A *uma matriz* $k \times (n-k)$*.*

Dado um código linear $\mathcal{C}$, nem sempre conseguimos encontrar uma matriz geradora de $\mathcal{C}$ na forma padrão. Contudo, se G é uma matriz geradora de $\mathcal{C}$, podemos permutar colunas de G, obtendo uma matriz G' que é a matriz geradora na forma padrão de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$.

Teorema 2.2 *Dado um código linear* $\mathcal{C}$*, existe um código* $\mathcal{C}'$ *equivalente a* $\mathcal{C}$ *que possui matriz geradora na forma padrão.*

2.1.3 Códigos duais

Definiremos nesta seção o código dual de um código linear $\mathcal{C}$. Esse código é fundamental no que diz respeito à verificação se determinada palavra em $\mathbb{K}^n$ pertence ou não ao código $\mathcal{C}$.

Dados $\mathbf{u} = (u_1, \ldots, u_n)$ e $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{K}^n$, define-se o produto interno de $\mathbf{u}$ e $\mathbf{v}$ por

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n.$$

Além disso, o produto interno satisfaz as propriedades de simetria

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$$

e bilinearidade

$$(\mathbf{u} + \lambda \mathbf{w}) \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} + \lambda(\mathbf{w} \cdot \mathbf{u})$$

para todo $\lambda \in \mathbb{K}$.

Seja $\mathcal{C} \subset \mathbb{K}^n$ um código linear. Define-se o conjunto ortogonal a $\mathcal{C}$ em $\mathbb{K}^n$ por

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{K}^n : \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{u} \in \mathcal{C}\}.$$

O conjunto $\mathcal{C}^{\perp}$ é um subespaço vetorial de $\mathbb{K}^n$ e, portanto, também é um código linear que chamaremos de **código dual** de $\mathcal{C}$.

Sejam $\mathcal{C}$ um (n, k)-código com matriz geradora G e $\mathbf{v} \in \mathcal{C}^{\perp}$. Então $\mathbf{v} \cdot \mathbf{c} = \mathbf{0}$, para todo $\mathbf{c} \in \mathcal{C}$. Logo $\mathbf{v}$ é ortogonal a todos os elementos de uma base de $\mathcal{C}$, o que equivale a dizer que $G\mathbf{v}^t = 0$, já que a matriz G é formada pelos vetores de uma base de $\mathcal{C}$. Assim podemos definir o código dual $\mathcal{C}^{\perp}$ da seguinte forma,

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{K}^n : G\mathbf{v}^t = \mathbf{0}\}.$$

Os resultados a seguir, que encerram essa seção, são obtidos através de aplicações de conceitos básicos de álgebra linear.

Proposição 2.2 *Seja $\mathcal{C} \subset \mathbb{K}^n$ um código de dimensão k com matriz geradora $G = (Id_k \mid A)$ na forma padrão. Então*

(i) $\dim \mathcal{C}^{\perp} = n - k$;

(ii) $H = (-A^t | Id_{n-k})$ *é uma matriz geradora de* $\mathcal{C}^{\perp}$;

(iii) $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

A proposição a seguir nos mostra como identificar se um elemento de $\mathbb{K}^n$ pertence ou não a um código $\mathcal{C} \subset \mathbb{K}^n$.

Proposição 2.3 *Sejam $\mathcal{C} \subset \mathbb{K}^n$ um código linear tal que $\mathcal{C}^\perp$ tem matriz geradora H e $\mathbf{v} \in \mathbb{K}^n$. Então*

$$\mathbf{v} \in \mathcal{C} \iff H\mathbf{v}^t = \mathbf{0}.$$

A proposição acima nos permite caracterizar os elementos de um código $\mathcal{C}$ por uma condição de anulamento. A matriz geradora H de $\mathcal{C}^\perp$ é chamada de **matriz teste de paridade** de $\mathcal{C}$. Com isso, os elementos de $\mathcal{C}$ ficam determinados por uma condição de anulamento, tendo um custo computacional baixo, pois basta determinar se $H\mathbf{v}^t$ é o vetor nulo de $\mathbb{K}^n$ para que $\mathbf{v}$ pertença a $\mathcal{C}$.

Como mencionamos no fim do Capítulo 1, dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros. Existe uma interdependência complexa entre os parâmetros de um código dado pelo teorema a seguir.

Teorema 2.3 (Cota de Singleton) *Os parâmetros $[n; k; d]$ de um código linear satisfazem à desigualdade*

$$d \leq n - k + 1.$$

Quando tivermos um código em que $d = n - k + 1$, chamaremos esse código de MDS (*Maximum Distance Separable*).

Exemplo 2.6 (Código de Hamming) *Um **código de Hamming** de ordem m sobre $\mathbb{F}_2$ é um código com matriz teste de paridade H_m de ordem $m \times n$, cujas colunas são os elementos de $\mathbb{F}_2^m \backslash \{0\}$ numa ordem qualquer.*

Portanto, sendo $\mathcal{C} \subset \mathbb{F}_2^n$ o código determinado pela matriz H_m, temos $n = 2^m - 1$, pela própria construção de H_m. Com isso, sua dimensão é $k = n - m = 2^m - m - 1$.

A distância mínima em um código de Hamming é $d = 3$.

Façamos um exemplo numérico para melhor ilustrar um código de Hamming. Considerando a matriz

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

temos $m = 3$, $n = 2^3 - 1 = 7$ e $k = 7 - 3 = 4$.

Proposição 2.4 *Todo código de Hamming é perfeito.*

Demonstração: Como $d = 3$, temos $\kappa = [\frac{d-1}{2}] = [\frac{3-1}{2}] = 1$. Dado $c \in \mathbb{F}_2^n$, temos

$$|D(c;1)| = n + 1.$$

Portanto,

$$|\bigcup_{c\in\mathcal{C}} D(c;1)| = [n+1]2^k = [2^m - 1 + 1]2^{n-m} = 2^n,$$

logo

$$\bigcup_{c\in\mathcal{C}} D(c;1) = \mathbb{F}_2^n$$

e o código é perfeito. ■

Um código de Hamming de ordem m é MDS se, e somente se, $m = 2$.

2.2 Anel de polinômios: códigos cíclicos

Considere a aplicação

$$\begin{array}{rcl} \sigma : \mathbb{K}^n & \to & \mathbb{K}^n \\ (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) & \mapsto & (c_{n-1}, c_0, c_1 \ldots, c_{n-2}). \end{array}$$

Chamaremos σ de **troca cíclica**. Um código linear $\mathcal{C} \subset \mathbb{K}^n$ é um ***código cíclico*** se $\sigma(c) \in \mathcal{C}$ para todo $c \in \mathcal{C}$, isto é, se $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, então $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

Exemplo 2.7 *O código* $\mathcal{C} = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ *é cíclico. Note que* $\mathcal{C}$ *é um subespaço vetorial de* $\mathbb{F}_2^4$ *e tem os seguintes parâmetros: comprimento* 4*, dimensão* 2 *e distância mínima* 2*.*

Para trabalhar com códigos cíclicos, o que faremos é dar a eles uma estrutura de anel, além da estrutura de espaço vetorial de $\mathbb{K}^n$, pois a partir disso poderemos fazer uso das propriedades dessa estrutura algébrica, o que será de grande ajuda, como veremos mais adiante.

Seja $\langle x^n - 1\rangle$ o ideal de $\mathbb{K}[x]$ gerado por $x^n - 1$ e defina R_n como o anel quociente dado por

$$R_n = \frac{\mathbb{K}[x]}{\langle x^n - 1\rangle}.$$

Assim, se $\overline{f(x)} \in R_n$, então

$$\overline{f(x)} = \{f(x) + g(x)(x^n - 1) : g(x) \in \mathbb{K}[x]\}$$

e as operações de adição e multiplicação são definidas respectivamente da seguinte maneira:

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}$$
$$\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)}$$

para quaisquer $\overline{f(x)}, \overline{g(x)} \in R_n$.

Temos também que R_n munido da multiplicação por escalar $\lambda \in \mathbb{K}$, dada por

$$\lambda\overline{f(x)} = \overline{\lambda f(x)}, \quad \forall\ \overline{f(x)} \in R_n$$

é um $\mathbb{K}$-espaço vetorial de dimensão n com base $\mathcal{B} = \left\{1, \overline{x}, \ldots, \overline{x^{n-1}}\right\}$ e, então, R_n é isomorfo a $\mathbb{K}^n$ e usaremos aqui o seguinte isomorfismo linear:

$$\begin{array}{rcl} \nu : \mathbb{K}^n & \to & R_n \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}}. \end{array}$$

Até aqui, vimos que R_n possui as estruturas de anel e espaço vetorial e que é isomorfo a $\mathbb{K}^n$, o que significa que todo código linear $\mathcal{C} \subset \mathbb{K}^n$ pode ser visto em R_n através do isomorfismo ν, o que nos permite usar ferramentas de anéis na busca de melhores algoritmos de codificação e decodificação.

2.2.1 Matrizes geradoras e teste de paridade de um código cíclico

Nesta seção, nosso objetivo é encontrar matrizes geradoras e matrizes teste de paridade para códigos cíclicos, mas primeiro vamos caracterizar estes códigos em R_n. Note que a troca cíclica em R_n é dada, através de ν, pela multiplicação de $\overline{f(x)}$ por $\overline{x}$. De fato, dado $\overline{f(x)} = \overline{c_0 + c_1 x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}} \in R_n$, temos que

$$\begin{array}{rcl} \overline{f(x)} \cdot \overline{x} & = & \overline{f(x) \cdot x} \\ & = & \overline{(c_0 + c_1 x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}) \cdot x} \\ & = & \overline{c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n} \\ & = & \overline{c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1}}. \end{array}$$

O lema e o teorema a seguir nos dão uma caracterização precisa dos códigos cíclicos em R_n.

Lema 2.1 *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $\overline{x}$.*

Teorema 2.4 *Um subespaço $\mathcal{C}$ de $\mathbb{K}^n$ é um código cíclico se, e somente se, $\nu(\mathcal{C})$ é um ideal de R_n.*

Demonstração: Seja $\mathcal{C}$ um subespaço vetorial de $\mathbb{K}^n$. Suponha que $\nu(\mathcal{C})$ é um ideal de R_n. Daí, pelo Lema 2.1, $\nu(\mathcal{C})$ é fechado pela multiplicação por $\overline{x}$ e, portanto, $\nu^{-1}(\nu(\mathcal{C})) = \mathcal{C}$ é um código cíclico.

Por outro lado, se $\mathcal{C}$ é um código cíclico, então vale a troca cíclica para $\nu(\mathcal{C})$ em R_n, isto é, $\overline{x} \cdot \overline{f(x)} \in \nu(\mathcal{C})$ para todo $\overline{f(x)} \in \nu(\mathcal{C})$. Logo, novamente pelo Lema 2.1 temos que $\nu(\mathcal{C})$ é um ideal de R_n.

■

Observe que para verificar se um subespaço vetorial $\mathcal{C}$ de $\mathbb{K}^n$ é um código cíclico sem a utilização do Teorema 2.4, seria preciso verificar se todas as trocas cíclicas pertencem a $\mathcal{C}$, o que poderia ser muito trabalhoso. Agora, é suficiente verificar se $\nu(\mathcal{C})$ é um ideal de R_n.

Um ideal no anel quociente R_n é da forma $\langle\overline{p(x)}\rangle$, onde $p(x)$ é divisor de $x^n - 1$. Então a partir de agora, $g(x)$ será sempre um divisor de $x^n - 1$ e ainda, denotaremos

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Teorema 2.5 *Seja $I = \left\langle\overline{g(x)}\right\rangle$ um ideal de R_n. Se $g(x)$ tem grau s, então temos que $\mathcal{B} = \left\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}\right\}$ é uma base de I como espaço vetorial sobre $\mathbb{K}$.*

Uma consequência direta do Teorema 2.5 é que se $I = \left\langle\overline{g(x)}\right\rangle$ é um ideal gerado como $\mathbb{K}$-espaço vetorial pela base $\mathcal{B}$, então fazendo $\mathbf{v} = \nu^{-1}\left(\overline{g(x)}\right)$, temos que $\mathcal{C}$ é gerado por $\{\mathbf{v}, \sigma(\mathbf{v}), \sigma^2(\mathbf{v}), \ldots, \sigma^{n-s-1}(\mathbf{v})\}$.

Corolário 2.2 *Seja $g(x)$ um polinômio divisor de $x^n - 1$ de grau s. Se $I = \left\langle\overline{g(x)}\right\rangle$ é um ideal de R_n, então*

$$\dim_{\mathbb{K}} I = n - s,$$

e o código $\mathcal{C} = \nu^{-1}(I)$ tem matriz geradora dada por

$$G = \begin{pmatrix} \nu^{-1}\left(\overline{g(x)}\right) \\ \nu^{-1}\left(\overline{xg(x)}\right) \\ \vdots \\ \nu^{-1}\left(\overline{x^{n-s-1}g(x)}\right) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \ldots & g_s & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_s & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & g_0 & \ldots & g_s \end{pmatrix}$$

Demonstração: Recorde que as linhas de uma matriz geradora de um código linear $\mathcal{C}$ são dadas pelos vetores da base. Neste caso, temos que $\mathcal{B} = \left\{\overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \ldots, \overline{x^{n-s-1}g(x)}\right\}$ é uma base para o ideal $I = \left\langle \overline{g(x)} \right\rangle$ de R_n e, utilizando a imagem inversa do isomorfimo ν, obtemos uma base para o código em $\mathbb{K}^n$.

■

Seja $p(x) = p_0 + p_1x + \cdots + p_tx^t$ um polinômio que divide $x^n - 1$. Chamaremos de **polinômio recíproco** de $p(x)$, o polinômio

$$p^*(x) = x^t f(x^{-1}) = p_t + p_{t-1}x + \cdots + p_0x^t. \tag{2.1}$$

Este polinômio também divide $x^n - 1$ e, portanto, é gerador de algum código cíclico. Quando consideramos o código cíclico gerado pelo polinômio recíproco de $h(x) = \frac{x^n-1}{g(x)}$ teremos um auxílio para encontrar uma matriz teste de paridade para o código cíclico $\mathcal{C}$ gerado por $g(x)$, como veremos no teorema a seguir.

Teorema 2.6 *Seja $\mathcal{C} = \nu^{-1}(I)$ um código cíclico, onde $I = \left\langle \overline{g(x)} \right\rangle$ é um ideal de R_n. Daí, $\mathcal{C}^\perp$ é cíclico e $\mathcal{C}^\perp = \nu^{-1}(J)$, onde J é o ideal de R_n gerado por $\overline{h^*(x)}$. Isto é, $J = \left\langle \overline{h^*(x)} \right\rangle$.*

Demonstração: Sejam $g(x) = g_0 + g_1x + \cdots + g_sx^s$ e $h(x) = h_0 + h_1x + \cdots + h_{n-s}x^{n-s}$. Note que o grau de $h(x)$ é $n - s$ e, portanto, $h_{n-s} \neq 0$. Considere as matrizes G e H a seguir:

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_s & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_s & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & g_0 & \ldots & g_s \end{pmatrix} \text{ e } H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \ldots & h_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & h_{n-s} & \ldots & h_0 \end{pmatrix}.$$

É fácil ver que as linhas de H são linearmente independentes. Seja $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ a base canônica de $\mathbb{K}^n$. Assim, a i-ésima linha de G é dada por

$$G_i = g_0\mathbf{e}_i + g_1\mathbf{e}_{i+1} + \cdots + g_s\mathbf{e}_{i+s},\ 1 \leq i \leq n - s,$$

e a j-ésima coluna de H^t é dada por

$$H_j = h_{n-s}\mathbf{e}_j + h_{n-s-1}\mathbf{e}_{j+1} + \cdots + h_0\mathbf{e}_{j+n-s},\ 1 \leq j \leq s.$$

Suponha que $i \leq j$. Daí, o produto interno de G_i por H_j é dado por

$$g_{j-i}h_{n-s} + g_{j-i+1}h_{n-s-1} + \cdots + g_0h_{j-i},$$

com $(j - i) \in \{0, \ldots, s - 1\}$. Note que a soma acima é o coeficiente de $x^{n-s+j-i}$ no produto $g(x)h(x) = x^n - 1$ e, como $1 \leq n-s+j-i \leq n-1$, temos que esse coeficiente obrigatoriamente

deve ser 0. O resultado é análogo se $j \leq i$.

■

Como $h^*(x)$ tem grau $n-s$ e divide x^n-1, com o Corolário 2.2 e o Teorema 2.6, podemos afirmar que o código $\mathcal{C}^\perp$ tem matriz geradora dada por

$$H = \begin{pmatrix} \nu^{-1}\left(\overline{h^*(x)}\right) \\ \nu^{-1}\left(\overline{xh^*(x)}\right) \\ \vdots \\ \nu^{-1}\left(\overline{x^{s-1}h^*(x)}\right) \end{pmatrix} = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & h_{n-s} & \dots & h_0 \end{pmatrix}$$

e, portanto, H é uma matriz teste de paridade para $\mathcal{C}$.

2.2.2 Codificação em códigos cíclicos

Sejam $\mathcal{C} \subset \mathbb{K}^n$ um código cíclico e considere o isomorfismo de $\mathbb{K}$-espaços vetoriais, onde $\mathbb{K}[x]_{s-1}$ é o espaço vetorial dos polinômios de grau no máximo $s-1$ a seguir:

$$\begin{aligned} \mu : \mathbb{K}^s &\to \mathbb{K}[x]_{s-1} \subset \mathbb{K}[x] \\ (c_0, c_1, \dots, c_{s-1}) &\mapsto \sum_{i=0}^{s-1} c_i x^i. \end{aligned}$$

Teorema 2.7 *Seja $\mathcal{C}$ um código cíclico. Suponha $\mathcal{C} = \nu^{-1}(I)$, onde $I = \left\langle \overline{g(x)} \right\rangle$, com $g(x)$ divisor de x^n-1. Seja R a matriz $(n-s) \times s$ cuja i-ésima linha é*

$$R(i) = -\mu^{-1}(r_i(x)),$$

onde $r_i(x)$ é o resto da divisão de x^{s-1+i} por $g(x)$. Então a matriz $(R \mid Id_{n-s})$ é uma matriz geradora de $\mathcal{C}$.

Demonstração: Sejam $q_i(x)$ e $r_i(x)$ o quociente e o resto da divisão de x^{s-1+i} por $g(x)$, respectivamente. Desta forma,

$$x^{s-1+i} = g(x)q_i(x) + r_i(x),$$

onde $r_i(x) = 0$ ou $r_i(x)$ tem grau menor ou igual a $s-1$. Sendo assim, $\overline{x^{s-1+i} - r_i(x)} \in I$, e esses vetores para $i = 1, \dots, n-s$ são linearmente independentes sobre $\mathbb{K}$. Como $\nu^{-1}\left(\overline{x^{s-1+i} - r_i(x)}\right) = \mathbf{e}_{s-1+i} - \mu^{-1}(r_i(x))$, onde $\mathbf{e}$ é vetor da base canônica de $\mathbb{K}^n$, temos que a matriz

$$\begin{pmatrix} -\mu^{-1}(r_1(x)) & 1 & 0 & \dots & 0 \\ -\mu^{-1}(r_2(x)) & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \\ -\mu^{-1}(r_{n-s}(x)) & 0 & 0 & \dots & 1 \end{pmatrix}$$

é uma matriz geradora de $\mathcal{C}$ e então $(Id_{n-s} \mid R)$ é uma matriz geradora de C na forma padrão. ■

Agora, veremos o algoritmo de codificação. Dado $(c_0, c_1, \ldots, c_{n-s}) \in \mathbb{K}^{n-s}$, esse vetor pode ser codificado como elemento de $\mathcal{C}$ como se segue:

$$(c_0, c_1, \ldots, c_{n-s})(R \mid Id_{n-s}) = (b_0, \ldots, b_{s-1}, c_1, \ldots, c_{n-s}),$$

onde

$$\begin{aligned}(b_0, \ldots, b_{s-1}) &= -c_1\mu^{-1}(r_1(x)) - \cdots - c_{n-s}\mu^{-1}(r_{n-s}(x)) \\ &= -\mu^{-1}(c_1 r_1(x) + \cdots + (c_{n-s}r_{n-s}(x)) \\ &= -\mu^{-1}\left(\sum_{i=1}^{n-s} a_i r_i(x)\right)\end{aligned}$$

Veja um exemplo para ilustrar melhor a ideia.

Exemplo 2.8 *Considere o polinômio $x^7 - 1$ sobre $\mathbb{F}_2$. A fatoração de $x^7 - 1$ é dada por*

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3).$$

Considere o código $\mathcal{C} \subset \mathbb{F}_2^7$ gerado por $g(x) = 1 + x + x^3$. Note que a dimensão do código é 4. Agora, vamos determinar uma matriz geradora desse código na forma padrão:

$$\begin{aligned}x^3 &= (x^3 + x + 1) + (x + 1) \\ x^4 &= (x^3 + x + 1)x + (x^2 + x) \\ x^5 &= (x^3 + x + 1)(x^2 + 1) + (x^2 + x + 1) \\ x^6 &= (x^3 + x + 1)(x^3 + x + 1) + (x^2 + 1).\end{aligned}$$

Sendo assim, pelo Teorema 2.7, uma matriz geradora de $\mathcal{C}$ é dada por

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Suponha que seja dado um vetor $(a_1, a_2, a_3, a_4) \in \mathbb{F}_2^4$, do código da fonte. Digamos, por exemplo, o vetor $(1, 1, 1, 0)$. Assim, de acordo com a discussão acima, a codificação desse vetor é

$$(b_0, b_1, b_2, 1, 1, 1, 0),$$

onde b_0, b_1 e b_2 são os coeficientes do polinômio

$$1 \cdot (1 + x) + 1 \cdot (x + x^2) + 1 \cdot (1 + x + x^2) + 0 \cdot (1 + x^2) = 0 + x + 0 \cdot x^2.$$

Portanto, a codificação de $(1, 1, 1, 0)$ é $(0, 1, 0, 1, 1, 1, 0)$.

CAPÍTULO 3

TEMAS PARA APROFUNDAMENTO

No cenário da teoria de códigos, o Brasil emerge como um terreno fértil para inovações, contribuindo com pesquisas que transcendem fronteiras e enriquecem a compreensão global dessas complexas estruturas matemáticas. Encerramos este material apresentando três áreas interessantes com representantes brasileiros: códigos de grupo, códigos algébricos geométricos e códigos e reticulados. É interessante destacar que para qualquer uma dessas áreas é indispensável uma breve revisão nas estruturas algébricas básicas de anéis, corpos e grupos e portanto sugerimos o bom livro introdutório de álgebra (GONÇALVES, 2017). E como já vimos, uma noção básica de álgebra linear também é fundamental no estudo de códigos, indicamos (HEFEZ; FERNANDEZ, 2016) ou (COELHO; LOURENCO, 2005) para uma boa revisão.

3.1 Códigos de grupo

Entre as bases que sustentam a álgebra, há dois assuntos que se destacam: a teoria de grupos e a teoria de anéis e álgebras, embora existam outros tópicos também importantes. No século XX, começou a se consolidar uma nova área de pesquisa em álgebra, apoiada nesses dois tópicos, que veio a ser conhecida como teoria dos anéis de grupo. A partir da segunda metade do século XX que a teoria começou a fixar suas principais questões e pervadir outras áreas da álgebra e mesmo outros campos das matemática. Um anel de grupo é uma estrutura híbrida entre as teorias de grupo e de anéis, que é definida como um módulo livremente gerado sobre um grupo com coeficientes em um anel associativo com unidade. A relevância da estrutura é que, entre outras coisas, é possível lançar-se mão das poderosas ferramentas de ambas as teorias, de grupos e de anéis, em seu estudo. Como já mencionado, no desenvolver da teoria de códigos, notou-se que a utilização de estruturas algébricas traria um ganho enorme. Neste contexto, a utilização de anéis de grupo geram o que chamamos de códigos de

grupo.

Sejam G um grupo e R um anel com unidade. Construiremos um R-módulo onde os elementos de G são uma base, e usaremos as operações de G e R para definir uma estrutura de anel sobre esse módulo.

Seja RG o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g,$$

em que $a_g \in R$ e $a_g = 0$, para quase todo $g \in G$, isto é, tem-se uma quantidade finita de coeficientes não nulos em cada soma.

Para dar a RG uma estrutura de anel, definimos a adição e a multiplicação como segue

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\alpha \cdot \beta = \sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g = \sum_{g,h \in G} a_g b_h gh.$$

Reorganizando os termos, podemos reescrever a multiplicação como

$$\alpha \cdot \beta = \sum_{u \in G} d_u u,$$

onde

$$d_u = \sum_{gh=u} a_g b_h.$$

Desta forma, RG é um anel com as operações descritas acima. Mais do que isso, RG é um anel com unidade $1 = \sum_{g \in G} u_g g$, onde o coeficiente correspondente à unidade do grupo é igual a 1 e $u_g = 0$ para todos os outros elementos de G.

Também podemos definir em RG a multiplicação de elementos de RG por elementos λ de R da seguinte forma

$$\lambda\alpha = \lambda \sum_{g \in G} a_g g = \sum_{g \in G} (\lambda a_g) g.$$

Com as três operações definidas acima, é possível verificar que RG é um R-módulo e, ainda, que se R é um anel comutativo, RG é uma R-álgebra.

Definição 3.1 *O conjunto RG, com as operações definidas acima, é chamado de* ***anel de grupo*** *de G sobre R. No caso em que R é comutativo, RG é chamado de* ***álgebra de grupo*** *de G sobre R.*

Como um anel de grupo, é, em particular um módulo, temos toda a estrutura da teoria de módulos para utilizar. Com isso, resultados clássicos como o Teorema de Wedderbun-Artin são importantes no desenvolvimento da teoria de códigos sobre essa nova estrutura. Para o leitor interessado em se aprofundar na teoria de módulos sugerimos (MILIES; SEHGAL, 2002).

Para comprrendermos um pouco melhor sobre o funcionamento dos códigos realizados sobre um anel de grupo vejamos um anel de grupo para um grupo abeliano finito sobre um corpo $\mathbb{K}$ tal que $car(\mathbb{K}) \nmid |G|$. Um estudo mais detalhado deste caso pode ser encontrado em (LUCHETTA, 2005).

Vamos ver o caso particular em que G é cíclico. Assumimos $G = \langle a : a^n = 1 \rangle$ e $\mathbb{K}$ um corpo tal que $car(\mathbb{K}) \nmid |G|$. Considere a aplicação $\theta : \mathbb{K}[x] \mapsto \mathbb{K}G$ dada por

$$f(x) \in \mathbb{K}[x] \mapsto f(a) \in \mathbb{K}G,$$

onde $\mathbb{K}[x]$ é o anel de polinômios sobre $\mathbb{K}$ na indeterminada x. É fácil verificar que θ é um epimorfismo de anéis. Portanto, pelo teorema do homomorfismo de anéis,

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{ker(\theta)}, \text{ onde } ker(\theta) = \{f(x) \in \mathbb{K}[x] : f(a) = 0\}.$$

Já que $\mathbb{K}[x]$ é um domínio de ideais principais, $ker(\theta)$ é o ideal gerado por um polinômio $f_0(x)$, de menor grau, tal que $f_0(a) = 0$. É importante observar que, sob este isomorfismo, o elemento a é levado na classe $x + \overline{f_0} \in \dfrac{\mathbb{K}[x]}{\langle f_0(x) \rangle}$.

Como $a^n = 1$, temos $x^n - 1 \in ker(\theta)$. Note que se $f(x) = \sum_{i=0}^{r} k_i x^i$ é um polinômio de grau $r \leq n$, então temos $f(a) = \sum_{i=0}^{r} k_i a^i \neq 0$, pois os elementos $\{1, a, a^2, \ldots, a^{n-1}\}$ são linearmente independentes sobre $\mathbb{K}$. Logo $ker(\theta) = \langle x^n - 1 \rangle$ e

$$\mathbb{K}G \simeq \frac{\mathbb{K}[x]}{\langle x^n - 1 \rangle}.$$

3.1.1 Código de grupo cíclico

Um **código de grupo** (à esquerda) de comprimento n é um código linear que é imagem de um ideal (à esquerda) de uma álgebra de grupo via um isomorfismo

$$\mathbb{K}G \to \mathbb{K}^n$$

que aplica G na base canônica de $\mathbb{K}^n$.

Definição 3.2 *Se G é um grupo de ordem n e $\mathcal{C} \subset \mathbb{K}^n$ é um código linear então $\mathcal{C}$ é um G-**código** (à esquerda) se existe uma bijeção entre a base canônica de $\mathbb{K}^n$ e G que se estende a um isomorfismo $\mathbb{K}^n \to \mathbb{K}G$ que aplica $\mathcal{C}$ em um ideal (à esquerda) de $\mathbb{K}G$.*

Assim, um código de grupo (à esquerda) é um código linear que é um G-código (à esquerda) para algum grupo G. De acordo com o tipo de grupo que estamos considerando, damos nomes mais específicos para estes códigos. Por exemplo, um **código de grupo cíclico** (ou abeliano, ou solúvel,...) é um código linear que é um G-código para algum grupo cíclico (ou abeliano, ou solúvel,...) G.

Em (COSTA, 2022) é possível encontrar um pouco mais de detalhes sobre os códigos de grupo cíclico, bem como uma análise sobre a importância de enxergar os códigos cíclicos sobre diferentes estruturas algébricas.

O estudo destes códigos de grupo tem obtido grande avanço nos últimos anos. E diversos autores têm se dedicado a obter resultados para diferentes tipos de grupo. Em (BERNAL; RÍO; SIMÓN, 2009), os autores trabalham com código de grupo para grupos que possuem uma certa decomposição em dois subgrupos abelianos. Em sua tese de doutorado, (ALDERETE, 2018), Alderete generaliza alguns dos resultados de Bernal, del Río e Símon para o caso de grupos que se decompõem em mais subgrupos abelianos.

Outro tópico interessante a se explorar neste contexto é a ponte entre a matemática pura e aplicada envolvida no assunto. Apesar das referências aqui indicadas serem basicamente de trabalhos de matemática pura, a área dialoga efetivamente com a área de engenharia. A obtenção de bons códigos é algo importante na teoria de informação. Sendo assim, obter bons parâmetros para os códigos estudados nas referências citadas é algo que parece promissor, especialmente para aqueles que aplicam a teoria matemática desenvolvida.

Atualmente no Brasil existem pesquisadores espalhados por diversas instituições com trabalhos na área de códigos de grupo, como por exemplo os professores Francisco César Polcino Milies, Thierry Petit Lobão, Raul Antônio Ferraz, Gladys Chalom, Marinês Guerreiro e Samir Assuena.

3.2 Códigos algébricos geométricos

Os códigos algébricos geométricos representam uma fascinante fronteira no campo da teoria de códigos, onde conceitos abstratos de álgebra se entrelaçam harmoniosamente com a geometria para criar ferramentas poderosas na transmissão segura e armazenamento confiável de informações digitais. Essa classe especial de códigos oferece uma abordagem inovadora para lidar com erros em sistemas de comunicação, proporcionando eficiência e robustez.

Em sua essência, os códigos algébricos geométricos combinam princípios da álgebra com a geometria algébrica para criar estruturas matemáticas que podem ser utilizadas na correção de erros. Álgebra, com suas operações sobre estruturas matemáticas, como corpos finitos, e geometria algébrica, que estuda as soluções de equações polinomiais, unem-se para formar um conjunto único de ferramentas que transcendem as barreiras tradicionais da teoria de códigos.

Ao contrário de abordagens mais convencionais, como os códigos de Hamming ou Reed-Solomon, que se baseiam principalmente em manipulações de bits, os códigos algébricos geométricos operam em espaços mais abstratos, utilizando polinômios e curvas algébricas para representar informações. Essa abstração oferece uma flexibilidade notável, permitindo a criação de códigos eficientes em termos de taxa e capazes de corrigir um número significativo de erros. Um bom material inicial para estudo dessa vertente da teoria de códigos é (FILHO; TAFAZOLIAN, 2021). O principal pesquisador de instituição brasileira na área de códigos envolvendo geometria algébrica foi o professor Fernando Torres, atualmente seus ex-orientandos e parceiros de pesquisas continuam atuando na área, destacamos por exemplo Gilberto Brito de Almeida Filho, Saeed Tafazolian, Cícero Carvalho, Wanderson Tenório e Guilherme Tizziotti.

Esses códigos têm uma ampla gama de aplicações, desde comunicações seguras até o armazenamento eficiente de dados em dispositivos digitais. Sua capacidade de lidar com erros decorre não apenas da detecção, mas também da correção, proporcionando robustez em ambientes propensos a interferências e degradação do sinal.

3.3 Códigos e reticulados

Uma outra vertente de estudo da teoria de códigos com bastante representantes no Brasil, é o estudo dos códigos explorando as propriedades das estruturas envolvidas numa abordagem, sempre que possível, geométrica. Neste contexto, o estudo dos reticulados vem se destacando.

Em 1900 o problema de determinar qual é o empacotamento esférico que cobre a maior parte do espaço foi categorizado como um dos problemas de Hilbert e isso veio a obter destaque na teoria da informação. Defini-se como densidade de empacotamento de um reticulado a proporção do espaço $\mathbb{R}^n$ coberto pelo empacotamento associado a este reticulado. O problema do empacotamento de esferas foi conectado à area dos códigos em um artigo de Claude E. Shannon em 1948, onde foi exibida a relação entre códigos corretores de erros e reticulados com alta densidade de empacotamento.

Definição 3.3 *Dado* $\{v_1, \ldots, v_m\}$ *um conjunto de vetores linearmente independentes em* $\mathbb{R}^n$*, definimos por reticulado o conjunto*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_1 v_1, \quad \lambda_i \in \mathbb{Z}, \quad \forall\ i = 1, 2, \ldots m \right\}.$$

Um empacotamento esférico no $\mathbb{R}^n$ é uma reunião de esferas de mesmo raio no $\mathbb{R}^n$ de modo que quaisquer duas esferas ou não se interceptam ou se interceptam apenas no bordo, enquanto um empacotamento reticulado no $\mathbb{R}^n$ é um empacotamento esférico cujo o conjunto dos centros das esferas forma um reticulado.

O uso de códigos e reticulados em teoria da informação vem sendo cada vez mais explorado e alguns pesquisadores brasileiros vem dedicando muitos de seus trabalhos ao tema, como por exemplo os professores Sueli Irene Rodrigues Costa, Marcelo Firer, Reginaldo Palazzo Junior, Marcelo Muniz Silva Alves, Antonio Aparecido de Andrade e Grasiele Cristiane Jorge. Inclusive alguns destes pesquisadores organizaram um excelente material introdutório para o assunto, (LAVOR; ALVEZ; ALL., 2012). Outra sugestão de material interessante para aqueles que se interessarem pelo o assunto é a tese de doutorado da professora Grasiele, (JORGE, 2012).

CONSIDERAÇÕES FINAIS

À medida que chegamos ao final deste minicurso, é apropriado refletir sobre essa breve introdução que apresentamos dos códigos corretores de erros. Nossa exposição começou com a formalização do conceito de códigos e uma breve contextualização histórica. Em seguida chegamos nos códigos mais utilizados na prática: os códigos lineares. Compreendemos que o uso da álgebra linear caracteriza essas estruturas fundamentais para a correção de erros em transmissões digitais. Em seguida, contemplamos os códigos cíclicos, destacando a utilização da estrutura de anéis no estudo destes códigos.

Ao adentrarmos o cenário brasileiro de pesquisas em códigos, fomos apresentados aos códigos de grupo, uma área rica em aplicações e fundamentada nas nuances da teoria de anéis de grupos. Comentamos sobre a relação entre a álgebra e a geometria ao explorar os códigos algébricos geométricos. Vimos como pesquisadores brasileiros, como Fernando Torres, estão na vanguarda dessa abordagem que utiliza propriedades geométricas para aprimorar a correção de erros em sistemas complexos. Finalmente, vimos um pouco sobre a área de códigos e reticulados. Nesta área a ênfase é dada nos aspectos geométricos dos códigos.

Esperamos que este minicurso tenha proporcionado uma compreensão introdutória dos códigos corretores de erros e suas diversas facetas. Os códigos permeiam nossa vida digital e desempenham um papel essencial na garantia da integridade das informações. Por fim, encorajamos os participantes a continuarem explorando este fascinante campo, seja em trabalhos de conclusão de curso, projetos de iniciação científica, mestrado e/ou doutorado.

REFERÊNCIAS BIBLIOGRÁFICAS

ALDERETE, S. A. *Códigos corretores de erros sobre grupos com decomposição m - abeliana*. Tese (Doutorado) — UFBA/UFAL, Bahia, 2018. 28

BERNAL, J. J.; RÍO, Á. del; SIMÓN, J. J. An intrinsical description of group codes. *Designs, Codes and Cryptography*, Springer, v. 51, n. 3, p. 289–300, 2009. 28

COELHO, F. U.; LOURENCO, M. L. *Um Curso de Álgebra Linear*. 2. ed. São Paulo: Ed USP, 2005. 25

COSTA, R. B. *Código de grupo cíclico*. 2022. Trabalho de conclusão de curso (Graduação em Licenciatura em Matemática),Departamento de Matemática Pura e Aplicada - CCENS, Universidade Federal do Espírito Santo. 10, 28

FILHO, G. B. de A.; TAFAZOLIAN, S. *Códigos Geométricos*. Rio de Janeiro: 33º Colóquio Brasileiro de Matemática, IMPA, 2021. 29

GONÇALVES, A. *Introdução à álgebra*. 6. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2017. 25

HEFEZ, A.; FERNANDEZ, C. d. S. *Introdução à Álgebra Linear*. 2. ed. Rio de Janeiro: Coleção PROFMAT, SBM, 2016. 25

HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. Rio de Janeiro: Instituto de Matematica Pura e Aplicada, 2008. 4, 8, 10

JORGE, G. C. *Reticulados q-ários e algébricos*. Tese (Doutorado) — IMECC - UNICAMP, Campinas, 2012. 30

LAVOR, C. C.; ALVEZ, M. M.; ALL. et. *Uma introdução à teoria de códigos*. São Carlos: Notas em Matemática Aplicada, SBMAC, 2012. 30

LUCHETTA, V. O. J. *Códigos cíclicos como ideais em álgebras de grupo*. Dissertação (Mestrado) — IME - USP, São Paulo, 2005. 27

MILIES, C. P.; SEHGAL, S. K. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, 2002. 27